(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 562 890 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **93302420.0**

(22) Date of filing : **29.03.93**

(51) Int. Cl.[5] : **H04Q 7/04,** H04B 7/26

(30) Priority : **27.03.92 GB 9206679**

(43) Date of publication of application :
29.09.93 Bulletin 93/39

(84) Designated Contracting States :
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant : **HUTCHISON MICROTEL LIMITED**
St. James Court, Great Park Road
Almondsbury, Bristol BS12 4QJ (GB)

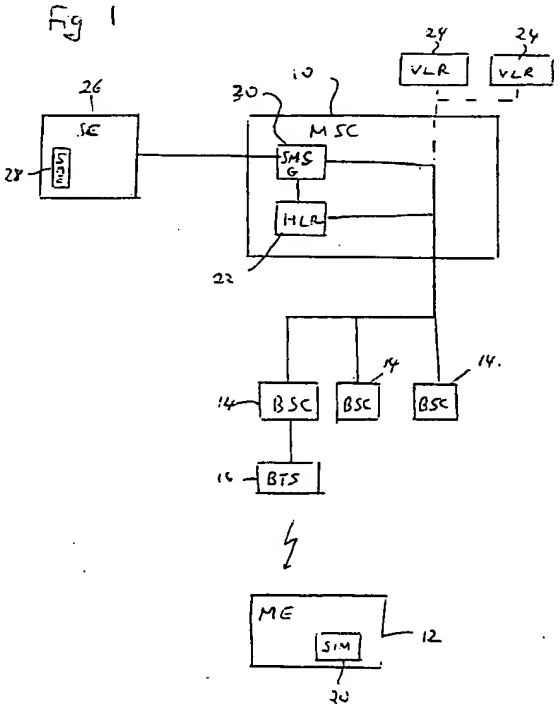
(72) Inventor : **Green, Steven**
96 Oakleaze Road
Thornbury Bristol BS12 1BP (GB)

(74) Representative : **Calderbank, Thomas Roger et al**
MEWBURN ELLIS 2 Cursitor Street
London EC4A 1BQ (GB)

(54) Mobile communication network with remote updating of subscriber identity modules in mobile terminals.

(57) A communications network has a switching network including a mobile switching centre (MSC 10) which communicates, e.g. by radio telephony, with mobile equipment (ME 12), such as a mobile telephone. The mobile equipment contains a subscriber identity module (SIM 20) which stores data for controlling the operation of, and the facilities available to the user, of the mobile equipment (12). In accordance with the present invention, the switching network transmits updating signals to the mobile equipment (12) which alter the data stored in the subscriber identity module (20), and hence alter the operation on facilities available.

Fig 1



EP 0 562 890 A1

The present invention relates to a mobile terminal for telecommunications, for example a portable telephone, and to a communications network making use of such terminals.

The use of mobile telephones is now increasing, and it is therefore increasingly desirable that the operation of a given mobile telephone is sufficiently adaptable for the user's needs.

At present, mobile telephones, particularly those based on the Groupe Speciale Mobile (GSM) Standards, contain an electronic module, known as a Subscriber Identity Module or SIM which stores data to be used by the mobile telephone. In the DECT standards, the corresponding module is known as a DECT authentication module (DAM). The term subscriber identity module or SIM will be used in this text to include both types of modules. The SIM is pre-configured to contain a unique identifier for a particular user, and may also contain appropriate authentication functions. The SIM is also able to store temporary data such as paging messages and a telephone number directory.

Currently, the SIM has a purely passive function within the mobile telephone, and stores data only. Apart from the temporary data, the software configuration of the SIM is entirely pre-determined by the organisation which supplies the SIM, which is normally the operator of the mobile communications network, or its appointed agent, in order that a given SIM may be configured according to the needs of a particular user. The disadvantage with this is that if the needs of the user change, the user must return the SIM to the supplier of the SIM, for re-configuration or a new SIM to be issued to the user. In the former case, the user is without a SIM for a period during which he is unable to use the services of the network, thus resulting in inconvenience for himself and loss of revenue to the network operator. In the latter case security risks arise with the user being potentially in possession of two SIMs both relating to his single subscription to the supplier.

Therefore, the present invention proposes that the data in the SIM is updatable by signalling from a central site, so that the SIM is re-configured by that data updating. The SIM then contains suitable software for processing commands received from the site to trigger that re-configuration.

Hence, the supplier may signal remotely to the SIM (which is straightforward since the SIM is located within a mobile telephone) and enables the supplier to change the functions of the SIM without the SIM having to be removed from the telephone.

Although the invention has been described above with reference to a mobile telephone, it is applicable to any terminal of a communications network making use of SIMs.

Thus, according to the present invention, operations which previously required the removal of the SIM from the mobile terminal, and its return to, or replacement by, the supplier, now may be achieved remotely. Of course, the SIM may be removed from any given mobile terminal and transferred to another mobile terminal, so that the user may transfer his use from one mobile terminal to another. Hence, the transfer of the SIM re-configures the mobile terminal according to the needs of the user. However, with the present invention, the configuration of the SIM itself may be changed according to changes in the needs of the user in any mobile terminal in which the SIM is located and which is arranged to embody the present invention.

It can be noted that it is believed that existing SIMs have sufficient memory to permit suitable software to be stored therein in order to achieve the present invention. However, it may be desirable to enhance the memory available in order to enhance the processing capability within a SIM for the invention to be facilitated, although any such enhancement must keep within the appropriate standards for the mobile terminal, e.g. the GSM standard.

An embodiment of the present invention will now be described in detail, by way of example, with reference to the accompanying drawings in which:

Fig. 1 shows a communication network in which the present invention may be embodied;

Fig. 2 is a flow chart showing the processing of a message by a SIM incorporating the present invention; and

Figs. 3a to 3c show the structure of messages which may be used in the present invention.

In Fig. 1 normal telephonic communication occurs between a switching network including a mobile switching center MSC 10 and a mobile telephone or other mobile equipment ME 12. Such communication is via one of a number of base station controllers BSC 14, each of which control a number of radio cells in which the ME 12 is located, and communicate with the ME 12 via a base transceiver system BTS 16.

The ME 12 contains a subscriber identity module or SIM 20 which stores pre-programmed data. A mobile equipment ME containing a SIM may be referred to as a Mobile Station MS or mobile Telephone. In particular, the SIM 20 stores a unique identifier of a particular user, and may also contain an authentication function.

Thus, when the SIM 20 is located in a given ME 12, the ME 12 is configured for use by the information in the SIM.

Immediately at the start of communication between the MSC 10 and the ME 12, the MSC checks whether the user is registered at the MSC itself, via a home location register HLR 22. If no match is found, the MSC 10 checks on one of a number of visitor location registers 24 which contain information used when a user is temporarily within the coverage of a MSC which is not the "home" MSC of the user.

In existing networks, it is possible to store a message in the SIM 20 of an ME 12. To do this, the supplier generates the message at a service center SC 26 of the switching network using part of the service center 26 known as a short message entity SME 28. The supplier therefore inputs the message via the SME 28 and the service center 26 transmits the message to the MSC 10 via a gateway SMSG 30 in the MSC 10. The message is then transmitted from the MSC 10 in the normal way to the ME 12, via the appropriate BSC 14 and BTS 16, and the message is stored in the SIM 20 of the ME 12. In practice, the ME 12 merely acts as a transferor of the message, and the message is passed to the SIM 20 in the form it was received from the MSC 10. The only function of the ME 12 in this operation is as a buffer. In currently defined practice, the only function of the message is to provide information to the user of the telephone via a textual display on the telephone. The message may thus be read, edited by the user, and sent to another user, or erased.

As described so far the system is conventional. As has previously been mentioned, the SIM 20 contains information identifying a particular user, and constraining that user to perform certain functions of the ME 12, and not others. This information is pre-programmed in the SIM 20. Thus, to take a simple case, the user may be prevented from making international calls, with appropriate data being stored in the SIM 20. However, if the user wants to change the functions available to him, he must return the SIM to the supplier for re-programming or request the issue of a new SIM. This imposes a delay on the changes in function which is undesirable, as well as creating security risks with the presence of two SIMs for one user subscription.

Therefore, the present invention proposes that the SIM 20 contain software which permits the SIM 20 to re-configure itself, in response to a suitable signal thereby changing the functions which it permits for the ME 12 in which it is located, and enables the SIM 20 to verify its changes with the network. The whole process of SIM reconfiguration and verification is done transparently to the user who may continue to use the telephone for normal calls, whilst the reconfiguration/verification process is happening. The process is also independent of the type of ME 12 and, as long as the ME 12 supports the GSM short message service, it can respond to a signal generated at the SME 28.

Thus, if the user wishes to change the functions available to him, he notifies the supplier accordingly and the supplier arranges, via the service center 26, for a suitable signal to be stored in the network, either at the service center 26, or the MSC 10. The MSC immediately tries to send a short message to the ME, without waiting for the ME to be activated. If this fails, due to the ME being switched off, the MSC will keep trying for a predetermined period, until successful otherwise, the next time the user uses the network, by activation of the ME 12, the MSC identifies such use by noting the unique identifier of the user associated with SIM 20, and immediately sends a signal to the ME 12 which causes the SIM 20 to re-configure itself according to the newly desired functions. Hence, very rapidly, the SIM 20 may perform the new functions requested by the user. Having re-configured itself, the SIM 20 carries out a verification process to ensure that the new configuration corresponds to that requested by the user. Verification involves the SIM 20 carrying out certain mathematical processes on its reconfigured data, comparing the results of this with the expected results as received from the network and advising the network of a satisfactory conclusion.

The re-configuration and verification process will now be described in detail. In the following description, it is assumed that the SIM is pre-programmed with standard or default commands, and all data stored has been initialised to known initial values. These operations will normally be carried out before the SIM 20 is issued to the user, by a suitable initialisation step. That initialisation step may also program PINs and other data such as the International Mobile Subscriber Identity (IMSI) data, the authentication key (Ki) data and the Pin Unblocking Key (PUK) data into the SIM.

Now suppose that a message is received by the SIM 20. This message may be a re-programming message, or it could be a conventional message which is stored at the SIM 20 and displayed to the user as previously described. Therefore, as shown in Fig. 2, the first step 100 when a message is received is to determine if the message is a remote SIM updating (RSU) message. If the message is not an RSU message, processing branches at step 101 to step 102, in which the message is stored in a suitable memory, such as a EEPROM of the SIM 20. The SIM 20 may then signal to the ME 12 that the message has been received, and this may be achieved at step 103 by returning a suitable status signal to the ME 12. With the message stored in the memory of the SIM 20, the processing stops at step 104, and the message may be displayed subsequently, with the display being triggered by a suitable input from the user.

If the message is determined to be an RSU message, branching at step 101 passes to step 105, in which the SIM 20 checks whether the updating function is enabled. This function will normally be enabled, but may be disabled for a particular SIM if that SIM is to be excluded from being updated according to the present invention. If it is disabled, the processing branches at step 106 to step 107 at which the message is converted to a textual message and processing then jumps to step 102, for display of the message as previously described.

If the RSU feature is enabled, however, the next step after the branching of step 106 is to carry out a check that the message has been received correctly. The present invention is not limited to any particular validation check method, but a simple method is to make use of checksum data in the message. In this arrangement, every message contains, in addition to other necessary information, checksum data which, when the information in the message is summed according to a predetermined rule, produces a zero result. Therefore, if the information is summed at validation step 107, and the result is not zero, the message has been received incorrectly. Thus, if the result of that validation check is not zero, processing branches at step 108 to step 110 in which a signal is generated from the SIM 20 to the ME 12 which indicates that there was a problem in the transmission of the RSU message. The SC 26 may then re-transmit the RSU message. If, however, the validation check of step 107 produces a zero result, processing branches at step 108 to step 109 in which the RSU message is analysed by the SIM to execute each command in the message. If, during the processing of step 110, an error occurs, processing branches at step 111 back to step 109, and the error is signalled to the SC 26 so that the RSU message is retransmitted. If every command is executed correctly, processing branches at step 111 to step 112 in which a message is generated to confirm that the processing of the RSU message has been completed. The message is stored in the memory of the SIM 20 in step 102.

Thus, it is possible to generate signals to the SIM 20 from the SC 26 which can cause the SIM to carry out specific commands. Each RSU message will therefore contain a series of commands, plus a checksum. The number of commands in the RSU message depends on the size of each command and is limited by the maximum size of the message function of the SIM 20.

The processing of the commands received by the SIM, after the checking process described with reference to Fig. 2 has been carried out, will now be described. As previously mentioned, each RSU message contains a series of commands plus a checksum. The first command in such a series has a security checking function, which will be described in more detail later. The other commands are those which update the SIM 20 in accordance with the present invention. Data is stored in a SIM in one of a plurality of fields, and there are two types of such fields. The first type is known as a "binary" field and consists of a single block of data, with the data within that block being unformatted (unstructured). An example of such data is the IMSI data referred to previously. The other type of field is a formatted field, and is a structured field consisting of a number of records, normally with a similar structure. In this embodiment of the present invention, the command carries new data to be overwritten into an appropriate binary or formatted field, together with data identifying that field. Thus, once the SIM 20 has confirmed that an appropriate RSU message has been received, using the processing of Fig. 2, then each command is processed by overwriting the data contained within that command into a field (either binary or formatted) identified within that command.

Fig. 3a shows the structure of a command for updating a binary field. As can be seen from Fig. 3a, the command has five elements. The first element nb is a coded representation of the total number of bytes (and hence the length) of the command. The second element is an identifier of the field in which the data is to be written. The third element is a coding element Ins, and then the length of data is identified. Finally, the data itself is carried within the command. Thus, the field into which the data carried by the command is stored in the Field ID element, and, once the field is identified, the data can be stored therein using standard processing operations known e.g. from the pre-configuration process.

Fig. 3b is a structure of a command for updating formatted data, it can be seen that the structure is effectively identical to that for updating a binary field.

As previously mentioned, the first command in a RSU message has a special function, in that it carries out a verification check, as previously mentioned, the updating function involves overwriting data in to one or more fields of the memory of the SIM 20, but for security such overwriting of the memory should occur only when the operator of the mobile communication network instructs such updating. Therefore, this embodiment proposes that the first command in the RSU message be a verifying command, the structure of which is shown in Fig. 3c. The general structure of this command is similar to that for updating the binary or record data, and consists of five separate elements. In fact, the data of this command is not to be written to a field, the Field ID data may be null. The data of this command then represents a code which is compared with a pre-recorded code within the SIM to act as validation.

Thus, each RSU message first enables access to the memory fields of the SIM by interaction of the validation command of Fig. 3c with an internal code of the SIM 20, and their successive commands can update binary and formatted fields by overwriting of data within the command into the appropriate field. Hence, the SIM can be updated remotely, and thus the network features available to the user of the ME 12 can be varied.

It may be noted that SIM 20 is normally removable from the ME 12 and is interchangeable amongst mobile terminals. Thus, the user is not limited to a particular terminal, provided he retains his own SIM 20.

It should also be noted that the conventional SIMs 20 contains sufficient memory space to store appropriate software, although that memory space has not previously been used for anything other than data storage of e.g. paging messages. However, in order that the existing functions of the SIMs 20 are not limited by the present invention, it may be necessary to increase the amount of memory space within the SIM 20, working within the limits imposed by the needs of the telecommunications network itself.

Claims

1. A mobile communications network comprising at least one switching network (10,26) and a plurality of mobile terminals (12), the at least one switching network (10) and each terminal (12) being arranged to transmit signals therebetween, each terminal (12) having a subscriber identity module (20) containing data for controlling the transmission of signals from the corresponding terminal (12) to the at least one switching network (10,26);
   characterised in that:
   the switching network (10,26) is arranged to transmit updating signals to at least one of said terminals (12) which alter the data of the subscriber identity module (20) of the at least one terminal (12).

2. A network according to claim 1 wherein the mobile terminals (12) are mobile telephones.

3. A network according to claim 1 or claim 2, wherein each subscriber identity module (20) has a memory comprising a plurality of fields storing said data, and each updating signal comprises information identifying one of those fields and information to be written into that one field, thereby altering said data.

4. A network according to any one of the preceding claims, wherein each subscriber identity module (20) is arranged to analyse each updating signal received to validate said updating signal prior to altering of the data of the subscriber identity module (20).

5. A mobile terminal (12) for a communication network having a subscriber identity module (20) containing data for controlling the transmission of signals from the mobile terminal (12), the data being stored in a plurality of memory fields;
   characterised in that:
   the terminal (12) is arranged to receive an updating signal comprising field information identifying one of the fields and second information to be written into that field, and is further arranged to alter the data in the field identified by the first information on the basis of the second information, whereby the data controlling said transmission is varied.

6. A method of operating a mobile communications network in which a plurality of mobile terminals (12) and at least one switching network (10,26) transmit signals therebetween, with the transmission of the signals from each terminal (12) to the at least one switching network (10,26) being controlled by a data in a subscriber identity module (20) within the corresponding terminal (12);
   characterised in that:
   the at least one switching network (10,26) transmits signals to at least one of the terminals (12) which alter the data of the subscriber identity module of the at least one terminal (12).

Fig 1

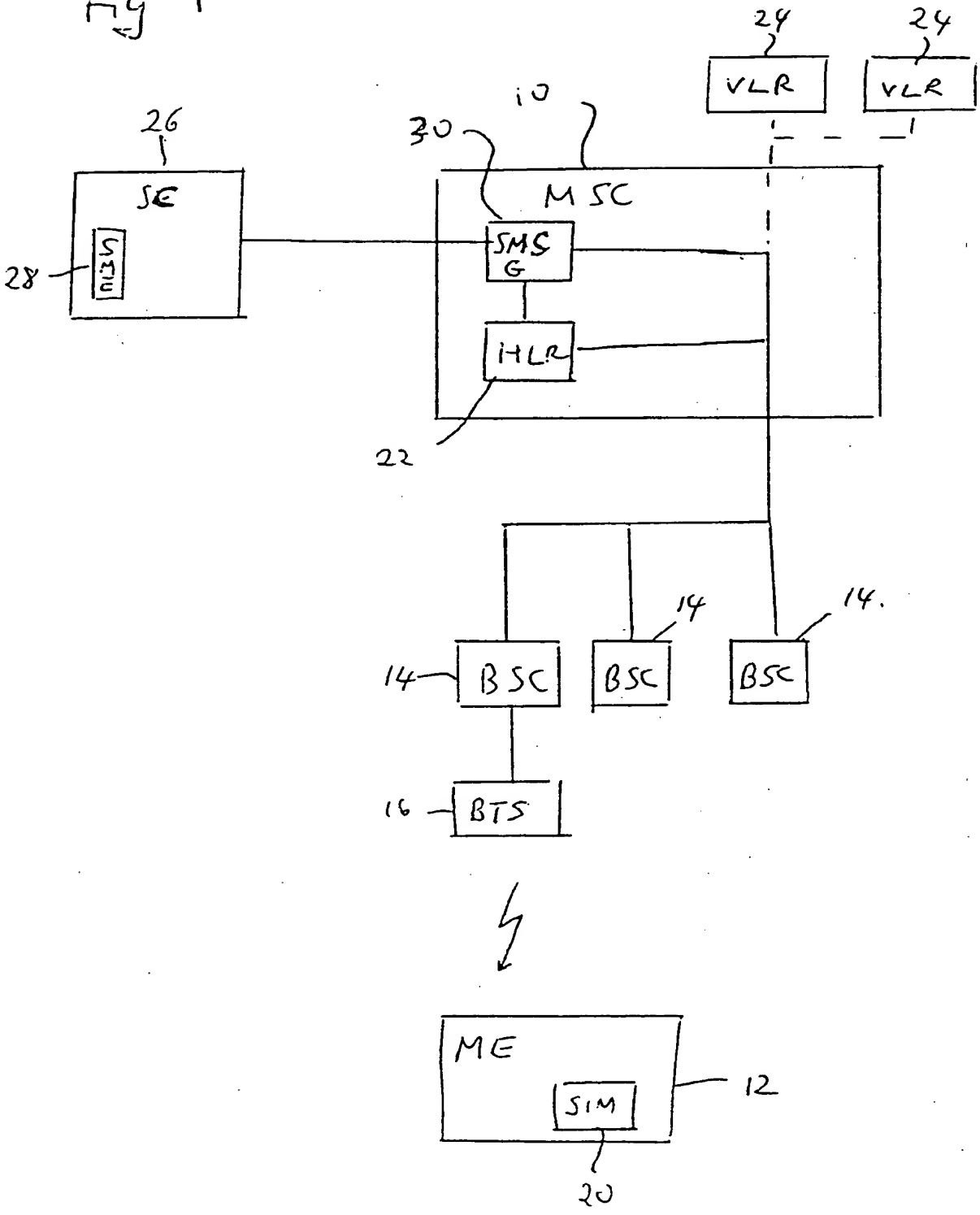

24
24
VLR
VLR
10
30
26
SE
MSC
SIM
28
SMS G
IHLR
22
14
14.
14
BSC
BSC
BSC
16
BTS
ME
SIM
12
20

Fig 2

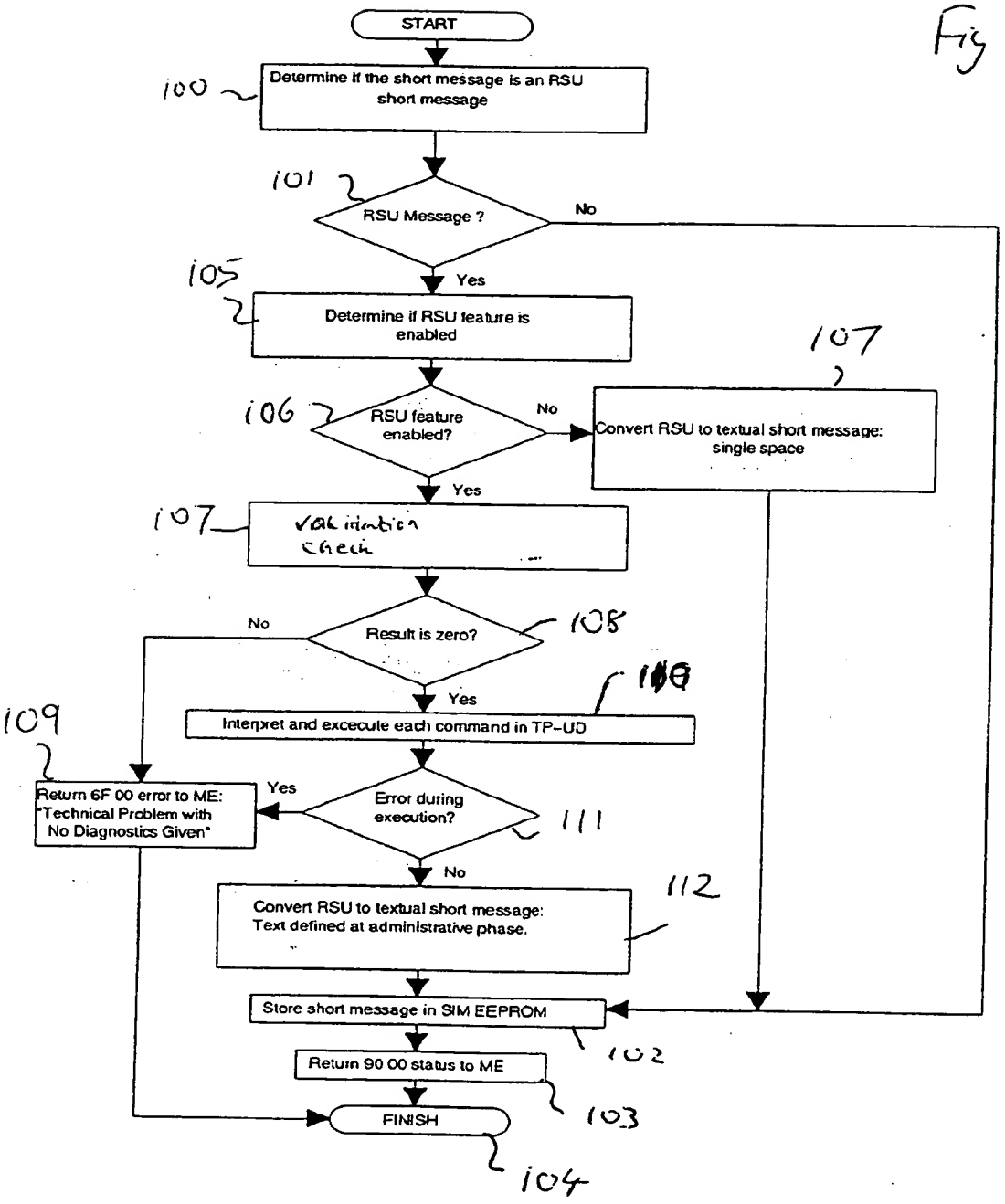

START
Determine if the short message is an RSU short message
100
RSU Message ?
101
No
Yes
Determine if RSU feature is enabled
105
RSU feature enabled?
106
No
Convert RSU to textual short message: single space
107
Yes
Validation check
107
Result is zero?
108
No
Yes
Interpret and execute each command in TP-UD
109
Return 6F 00 error to ME: "Technical Problem with No Diagnostics Given"
Yes
Error during execution?
111
No
Convert RSU to textual short message: Text defined at administrative phase.
112
Store short message in SIM EEPROM
102
Return 90 00 status to ME
103
FINISH
104

Fig 3a

nb	Field ID	Ins	Data Length	Data
Number of bytes in this command.	Data–field ID (4 bytes).	3 bytes	Length of data.	Data.

Fig 3b

nb	Field ID	Ins	Data Length	Data
Number of bytes in this command.	4 bytes	3 bytes	Length of data.	Data.

Fig 3c

nb	Field ID	Ins	Data Length	Data
Number of bytes in this command. Always 0F.	(FF FF).	3 bytes	Length of data. (08)	Data (8 bytes).

European Patent Office

EUROPEAN SEARCH REPORT

Application Number EP 93 30 2420

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
X	US-A-5 046 082 (ZICKER ET AL.) * column 3, line 43 - column 4, line 4 * * column 8, line 35 - line 48 * * column 16, line 27 - column 19, line 47 * * column 28, line 3 - line 21 *	1-6	H04Q7/04 H04B7/26
X	EP-A-0 459 065 (ETAT FRANCAIS) * column 2, line 9 - column 7, line 21 * * column 9, line 5 - line 33 * * column 13, line 11 - column 15, line 58 * * column 16, line 37 - line 45 *	1-6	
A	EP-A-0 459 344 (ALCATEL CIT) * column 1, line 47 - column 2, line 16 * * column 2, line 45 - column 3, line 51 * * column 4, line 56 - column 5, line 40 *	1-6	

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	25 JUNE 1993	BEHRINGER L.V.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

Fig 1

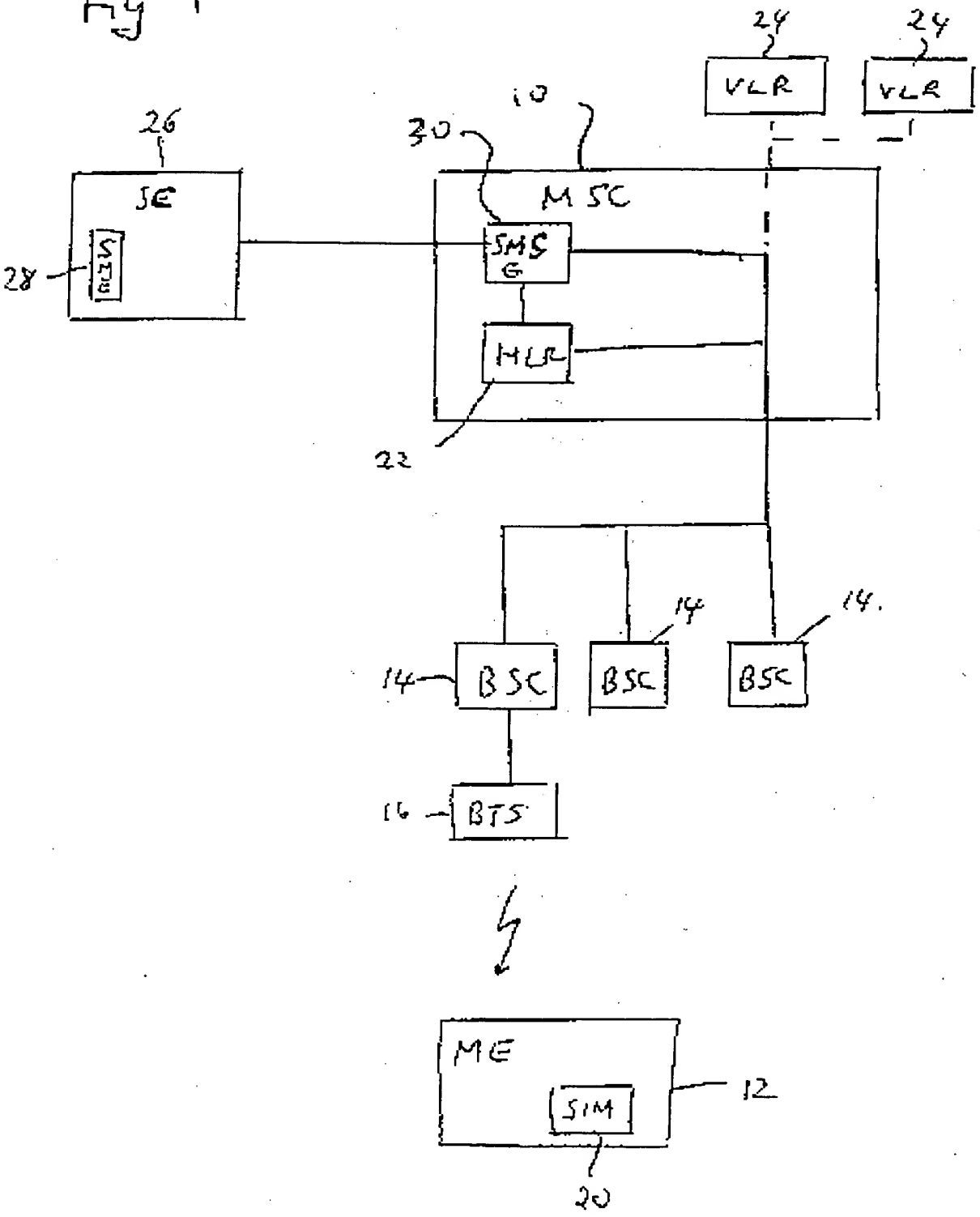

24
24
VLR
VLR
10
30
26
SE
MSC
SMS
G
28
SMS
G
HLR
22
14
14
14.
BSC
BSC
BSC
16
BTS
ME
SIM
12
20

Fig 2

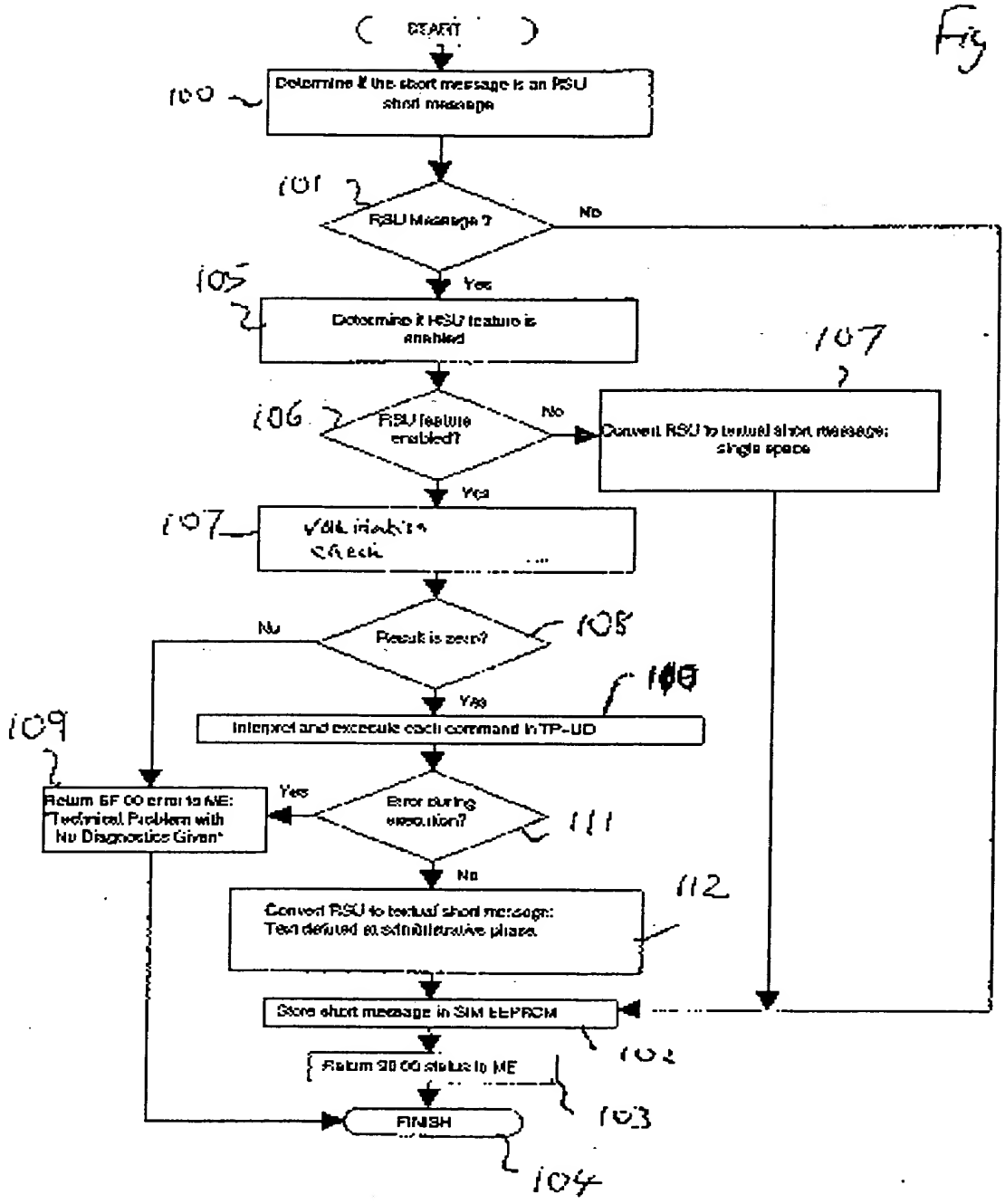

START
100
Determine if the short message is an RSU short message
101
RSU Message ?
No
Yes
105
Determine if RSU feature is enabled
106
RSU feature enabled?
No
Yes
107
Convert RSU to textual short message: single space
107
Validity check
Result is zero?
No
Yes
108
Interpret and execute each command in TP-UD
109
Return SF 00 error to ME: "Technical Problem with No Diagnostics Given"
Yes
Error during execution?
111
No
112
Convert RSU to textual short message: Text defined at administrative phase
Store short message in SIM EEPROM
102
Return 90 00 status to ME
103
FINISH
104

Fig 3a

nb	Field ID	Ins	Data Length	Data
Number of bytes in this command.	Data-field ID (4 bytes).	3 bytes	Length of data.	Data.

Fig 3b

nb	Field ID	Ins	Data Length	Data
Number of bytes in this command.	4 bytes	3 bytes	Length of data.	Data.

Fig 3c

nb	Field ID	Ins	Data Length	Data
Number of bytes in this command. Always 0F.	(FF FF).	3 bytes	Length of data. (08)	Data (8 bytes).